# Does Mobile Processing Scare You?

# It Should.

*The risks of mobile processing and best practices for secure payment transactions*

securityMETRICS®

# Contents

# About This eBook

## Who should read this eBook?

- Businesses that currently use mobile device payment processing (mPOS)
- Businesses considering mPOS solutions
- Financial institutions that offer mPOS products and services
- Individuals concerned about the security of their payment data in mPOS transactions

## What does this eBook include?

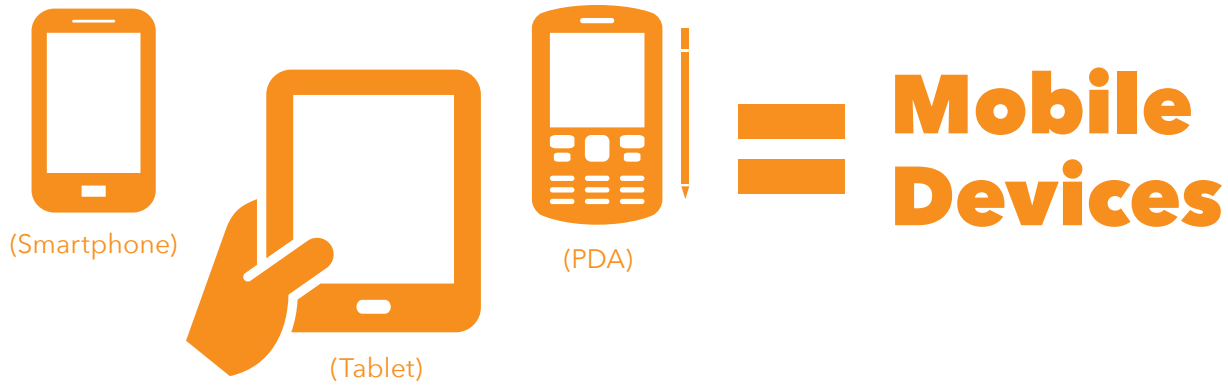
- A brief background of the mobile device and mobile processing industries
- Current security risks mPOS presents to both consumers and businesses
- How criminals use mobile vulnerabilities, malware, and malicious apps to steal personal data
- Current best practice guidelines for businesses that wish to securely implement a mPOS solution

## Why was this eBook written?

The mission of this eBook is to explain the risks of processing payments via mobile devices through data, statistics, and case studies, and provide best practice solutions to protect mobile transactions.

# Introduction

Mobile processing has been hyped as the future of payment transactions; but as the number of businesses using mobile point-of-sale (mPOS) solutions increase, so does the challenge of securing mobile devices.




Most people mistakenly believe mobile devices are already secure. In actuality, mobile devices have inherent security flaws that may put merchant transactions at risk of compromise.

If you use smartphones or tablets for mobile processing, the time to secure those devices is now. This introductory guide will walk you through the basics of mobile payments and offer best practices to fortify mobile transactions.

Let's get started.

01 Chapter

# The Mobile Ecosystem

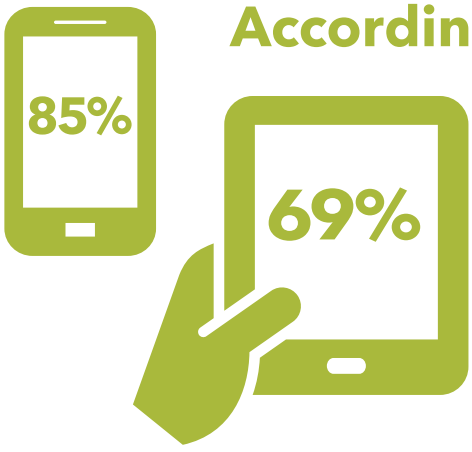
## World Domination

Consumers are buying mobile devices faster than ever. It's predicted that nearly 1.25 billion smartphones and tablets will be purchased in 2013 alone*. With Earth's population at a whopping 7 billion, that will mean one mobile device for every five people in the world.

**The average person checks their smartphone every 6.5 minutes!**

## Market Ownership

Quick! Name the major operating systems that dominate the mobile space today! If you said Apple® iOS and Google Android™, you're spot on. While Apple is one of the world's most profitable companies, when it comes to mobile platforms, Android is the big kahuna. 1.3 million Android devices are activated every day, which means every 24 hours more than four times as many mobile devices are set up than babies are born.




**According to a recent AT&T survey:**

**85% of small businesses use smartphones for operations**

**69% of small businesses use a tablet computer**



** Estimate based on CCS Insight and IDC findings.*

## 2012 Smartphone Market Share

**Android** 69%

**iOS** 19%

**BlackBerry®** 5%

**Windows®** 3%

## Apps, Apps, and More Apps

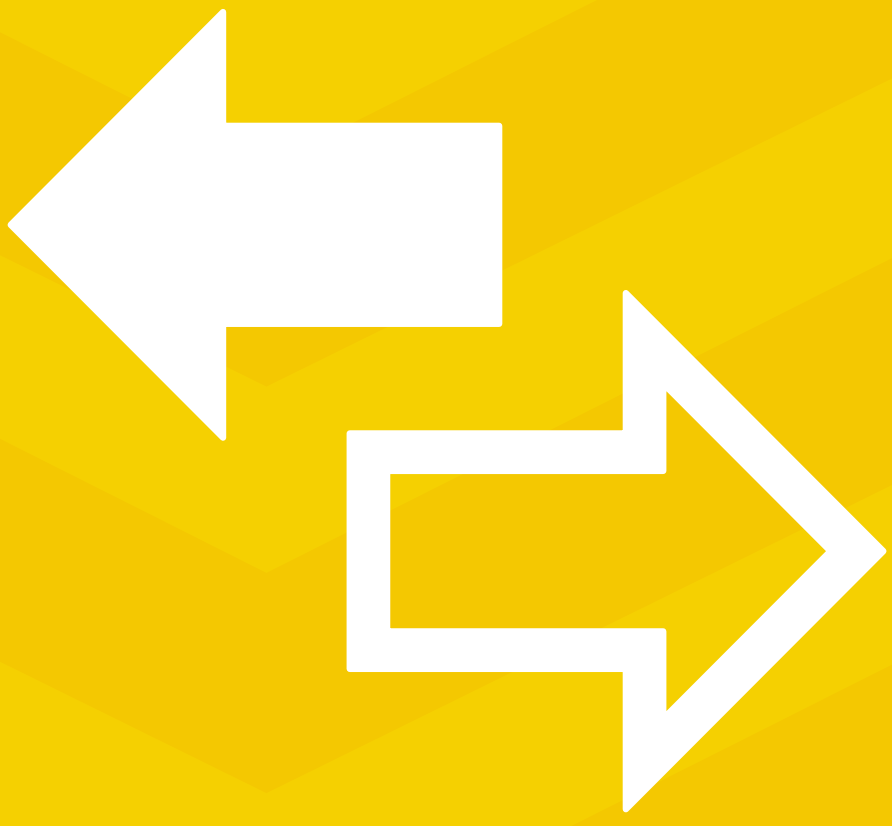
The average smartphone contains 41 apps that its owner uses on a regular basis. We used to rely on mobile devices for things like communication and planning, but now they are more like virtual Swiss Army knives. Creative developers release more app functionality each year, including the ability to start cars remotely, measure your heart rate, dim house lights from 50 miles away, and even act as a virtual cash register.

**50 BILLION**

**Total number of unique downloads that both Apple's App Store and Android's Google Play will reach in 2013.**

02 Chapter

# Mobile Processing



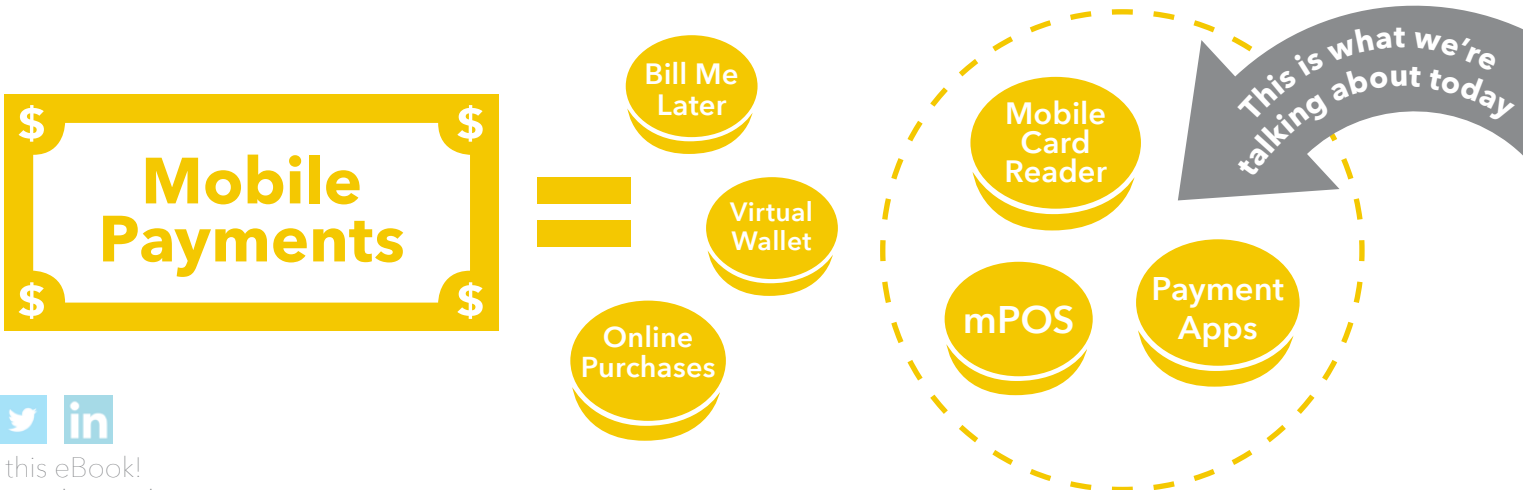
**By 2015, it is estimated that mPOS could increase new card payments by $1.1 trillion.**

## Mobile Processing

Mobile processing is a very simple and flexible way for merchants to process payments. An easy way to think of mobile processing is that it enables every smartphone or tablet to be its own swipe terminal. Merchants attach hardware to a smartphone or tablet that reads the data from a card's magnetic stripe, or use a payment processing app to manually enter card data. Notable mobile processing solutions include GlobalBay Mobile POS™, Square®, and Intuit® GoPayment. Many traditional processing banks also offer mobile solutions.

## Growth of Mobile Processing

Mobile is changing the entire shopping experience for both consumers and merchants. Initially, mPOS was adopted by micro-merchants (e.g., photographers, tradesmen, dog groomers) with low-value transactions. Compared to legacy payment systems, mobile POS solutions are cost effective, convenient, and easy to implement. Now, mobile payments have exploded beyond the niche market of micro-merchants to large global brands.



## Customer Confidence in mPOS

Customers are still quite wary of how mobile processing could affect their privacy and personal data. In fact, only 28% of consumers consider mobile processing to be secure. With recent news reports of high profile data breaches, it's no wonder consumers question mobile payment processing.

However, it is widely felt that mPOS will soon break the dam of caution that blocks consumer confidence in mobile processing. Square, a mobile processing service, has reported exponentional growth over the past few years. A similar growth pattern could undoubtedly be applied to other mPOS solutions. Small businesses are adopting mobile technology in increasing numbers. In fact, of businesses that use mobile devices, one out of five use them to accept payments.

**Square payment card transactions increased 3,200% in the last 24 months.**

03 Chapter

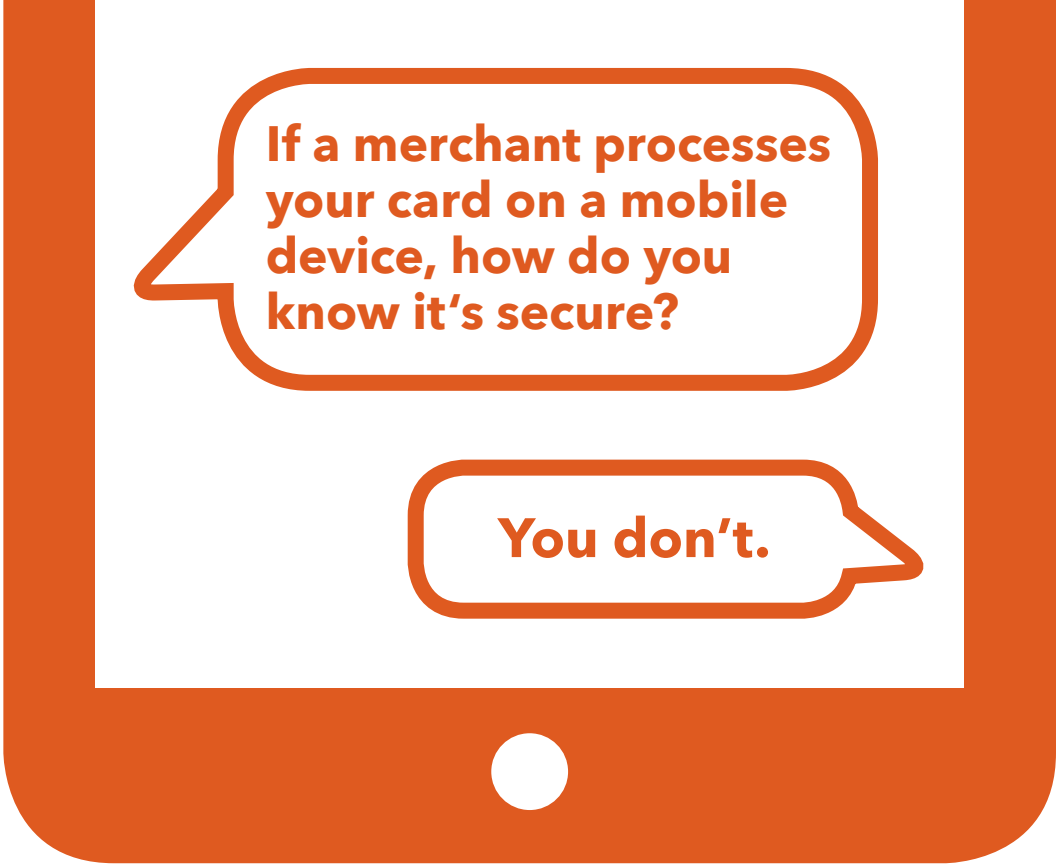
# Security Issues

## Just Like Computers, But...

Boiled down, mobile devices are sophisticated computers that lack many features of computer security. The problem is, smartphones and tablets have similar threats as a desktop or laptop, such as malware, insecure environments, and communication attacks, but lack the fortification to thwart attacks. Scared yet?


Since mobile technology is extremely powerful, people mistakenly assume mobile devices are as secure as a typical hardware point-of-sale (POS) system. POS systems are typically placed behind a firewall in a controlled environment with limited access to the Internet, and therefore have limited attack vectors; whereas mobile devices are automatically connected to the Internet via cellular or unsecured public wireless. Mobile devices don't include firewalls or other safeguards, and are wide open to potentially hostile environments.

Essentially, mobile devices were designed for convenience and ease of use, not necessarily for security.




## Your Data: A Hacker's Gold Mine

Mobile devices handle a lot of sensitive material. Traditionally, mobile hackers profited from the personal information of you and your contacts. However, with the rise of mobile credit card processing and financial management apps, a more valuable set of information has become available to steal—credit card data. It won't be long until hackers begin to take notice.

If that makes you a little unnerved, it should seriously alarm you to learn that 32% of mobile malware created in 2012 was designed to steal information from your device. Luckily, there hasn't been a large number of mobile breaches reported…yet. However, it's just a matter of time.

## Mobile Malware

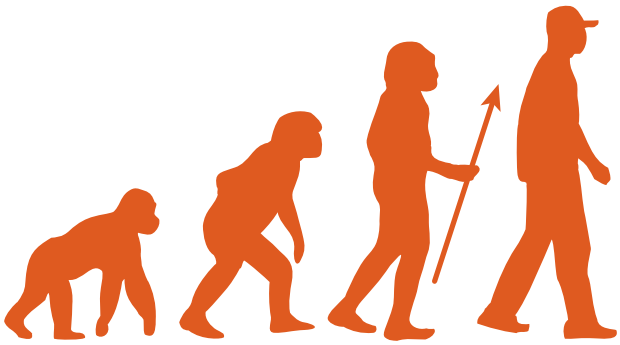
Mobile malware is bad news for smartphone and tablet users. Mobile malware are packages of software that carry out malicious activities on a mobile device, and the amount of mobile malware is growing daily.

**It's gonna be a long year... Over 40K unique malware threats were created in 2012. The first quarter of 2013 has already seen 22K new threats.**

How worried should you be? That depends what type of mobile platform you use.

Google has a target painted on its mobile platform. In 2012, over 97% of all the malware in the world was designed specifically for Android. Why is everyone picking on Android? Well, one reason is its app store. Compared to Apple's App Store, Google Play™ places fewer restrictions on development, which is great for writing apps, but terrible for security. An Android app can access data outside of its own application, which allows hackers to create malicious malware designed to compromise mobile security.

Don't rejoice just yet iOS and Windows users. It isn't as easy to write malware for iOS, but it happens. If we know one thing about hackers, it's that they evolve. As mobile transactions and the opportunity for fraud increases, hackers will become more sophisticated in their attacks (as hackers always do).



## Evolution of Hackers

**Expect more creative attacks as hackers evolve. For example, researchers recently discovered a way to hack Apple devices through malicious chargers.**

# Types of Mobile Malware

Let's look at common ways malware ends up on mobile devices.

## Apps

Malicious apps are the most common type of mobile malware. Criminals write apps with malicious code, or secretly add lines of code into legitimate apps and reload them into the app marketplace for unsuspecting victims to download. Newly installed apps packaged with mobile malware are fully functional, but also deviously work in the background to collect personal data, change settings, remotely control the device, or even read from unencrypted card readers attached to your smartphone or tablet.

Want proof? Here are a few examples.

- A single piece of malware was downloaded over 2 million times via 32 different apps from 4 separate developer accounts. The malware signed users up for a paid SMS service and directed users to download infected apps that hijacked their mobile devices.
- A piece of malware was inserted into a wallpaper app that secretly captured phone tones with the intelligence to report any data from manually typed credit cards.
- Malware was developed that enabled the user's phone to continue downloading malicious data indefinitely. In other words, after the app was downloaded, the malicious possibilities were endless–even if the app was removed. This piece of malware was downloaded 200,000 times in four days.

## URLs

Malware developers use malicious URLs to collect personal information. A malicious URL redirects a user to a fraudulent site in hopes they will enter sensitive information, such as a password, mobile number, or social security number. Guess what? It works. This year, 4 in 10 mobile users will click an unsafe link on a smartphone. Because smartphone and tablet screens are significantly smaller than computer screens, malicious links are easier to hide between lines of harmless text.


**Hackers also use SMiShing, where cybercriminals encourage consumers to click on malicious links via text message.**

**More than 800 apps are downloaded per second. How many of those apps are infected with malware?**

## Operating System Vulnerabilities

Because smartphones and tablets were never designed for data security, mobile operating systems have inherent flaws that automatically make them less secure than computers. Why does your smartphone constantly alert you to download the latest software update? It is likely because smartphone makers have found a security hole in the operating system and have to patch it with an update.

Here's where the lack of security rears its ugly head. Operating system security holes stay open for a variety of reasons. Some mobile platforms don't alert users of updated versions. Quite often, users ignore the update. Check out this statistic. Two years and two operating systems later, more than 39% of Android users are still using the Gingerbread operating system. For those not familiar with Android, Gingerbread is the version 2.3 platform of Android from 2010. As a result, these mobile consumers are lacking many of the major security updates provided by Ice Cream Sandwich and Jelly Bean. Yikes!

04 Chapter

# Protecting Mobile Processing

## The Evolution of Mobile Hardware

Security will continue to evade mobile processing until mobile manufacturers make security changes in hardware and operating system software. Some new smartphones are being released with dual processors, which allows for segmentation of processing activities from other apps, the Internet, and texting capabilities. New iPhones are rumored to have stricter security protocols to protect mobile payments. However, until phones and tablets are created specifically with security in mind, true mobile processing security will continue to be a gamble.

## Mobile Regulations

The Payment Card Industry Security Standards Council (PCI SSC) is the organization responsible for defining processing security requirements. The PCI SSC has provided **mobile payment acceptance guidelines** to help businesses process mobile transactions securely.

## Best Practices

The safest scenario for merchants who wish to accept mobile payments is to use an encrypt-at-swipe (or encrypt-at-type) reader, which encrypts card information before it enters the device and the mobile processing service decrypts it after it leaves. Even if a criminal gains access to the mobile device, all they would receive is a useless string of ciphertext. Note that many of the early mPOS card readers like Square and GoPayment didn't have encryption as a feature, so users should perform due diligence to ensure their dongles have been upgraded to the encrypted model.

Some mPOS vendors offer solutions in which the swipe reader is optional. Experts have counseled against manually entering credit card numbers, as the lack of encryption may allow a rogue app to intercept the card data.

## Mobile Vulnerability Scanning

One part of securing a mobile platform is to scan it for mobile vulnerabilities. **SecurityMetrics MobileScan** is an app that scans devices internally to help users avoid threats that originate from things like mobile malware and unwarranted app privileges. Because it was designed for businesses, MobileScan was created using the PCI Mobile Payment Acceptance Security Guidelines.

# Top 7 Best Practices

1. Use an encrypt-at swipe hardware reader created by a big player in the mPOS field (e.g., Square).
2. Minimize the manual entry of credit cards.
3. Read and follow the PCI SSC Mobile Payment Acceptance Security Guidelines.
4. Ensure everyone who comes in contact with the device (e.g., employees) is educated on mobile security.
5. Only download apps from official app stores (e.g., Google Play, Apple App Store).
6. Stay up to date with both app and operating system software.
7. Download and begin using a mobile vulnerability scanning app on your mobile processing device (e.g., SecurityMetrics MobileScan).

05 Chapter

# Summary

## Make Changes Now

As the number of businesses processing on mobile devices begins to rise, hackers will begin targeting mobile transactions. Should the security risks of mobile processing concern you? Yes. Should the security risks stop you from processing customer credit cards on mobile devices? No, as long as you take the necessary precautions like using encrypt-at-swipe/type readers, avoiding manual data entry, and scanning mobile devices for vulnerabilities.

Luckily, a significant mobile breach of credit card data hasn't yet been reported, but it's just a matter of time. Until mobile hardware is altered, simple security precautions must be taken to secure customer's sensitive data. If you identify the current risks inherent to your mobile devices and make necessary changes today, you may prevent the serious mobile security problems of tomorrow.

## Protect Yourself With MobileScan


mobilescan@securitymetrics.com

www.securitymetrics.com/mobilescan

# About SecurityMetrics

SecurityMetrics protects e-commerce and payments leaders, global acquirers, and their retail customers from security breaches and data theft. The company is a leading provider and innovator in merchant data security, and has helped over 1 million organizations as an Approved Scanning Vendor and Qualified Security Assessor.

Among other products and services, SecurityMetrics offers PCI audits, PA-DSS audits, security consulting, mobile device vulnerability scanning, penetration testing, data discovery tools, and forensic analysis.

Founded in October 2000, SecurityMetrics is a privately held corporation headquartered in Orem, Utah, USA.